

Juin 2008

Transferts de données à caractère personnel vers des pays non membres de l'Union européenne

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00



SOMMAIRE



A quelles conditions le transfert peut-il s’effectuer ?

- **Le principe : la nécessité d’une protection suffisante dans le pays d’établissement du destinataire**

L’article 25 de la directive 95/46 et l’article 68 de la nouvelle loi prévoient qu’un responsable d’un traitement ne peut transférer des données à caractère personnel vers un État n’appartenant pas à la Communauté européenne (dit « pays tiers ») **que si cet État assure un niveau de protection adéquat ou suffisant** de la vie privée et des libertés et droits fondamentaux des personnes à l’égard du traitement dont ces données font l’objet ou peuvent faire l’objet.

La Commission européenne a le pouvoir de reconnaître qu’un pays accorde une protection adéquate ou suffisante, dans une décision prise à cet effet, dénommée « décision d’adéquation ». A ce jour, la Commission européenne a pris plusieurs décisions dans ce sens.

> **A consulter**
>
> *Sur le site de la Commission européenne :* Décisions de la Commission européenne relative à la constatation du caractère adéquat de la protection des données dans les pays tiers.
>
> *Se reporter à :* « Pays équivalent », « pays adéquat », « pays non adéquat » : quel est le statut des législations de protection des données personnelles dans le monde ?

Les transferts de données à caractère personnel vers les destinataires entrant dans le champ d’application de telles décisions d’adéquation ne doivent faire l’objet d’aucun encadrement spécifique (contrat, règles internes, etc.).

La CNIL n’a pas à autoriser les transferts vers des pays accordant une protection adéquate. Elle devra cependant être informée de l’existence de ces transferts dans le cadre des formalités préalables à la mise en œuvre du traitement principal dont ces transferts sont issus (sur ce point, se reporter à la question 12).

- **Exception au principe : transfert autorisé par la CNIL sur la base d’un contrat ou de règles internes**

La CNIL peut également autoriser un transfert vers un pays tiers ne disposant pas d’un niveau de protection adéquate lorsque « le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des **clauses contractuelles** ou **règles internes** dont il fait l’objet » (article 69 al.8 de la loi du 6 janvier 1978).

Cette disposition est désormais la règle en matière de transferts internationaux de données vers des pays n’accordant pas une protection considérée comme adéquate.

La CNIL doit porter à la connaissance de la Commission européenne et des autorités européennes de contrôle les décisions d’autorisation de transfert de données à caractère personnel qu’elle prend au titre de l’article 69 alinéa 8.

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00



Se reporter à :

Quel contrat utiliser pour encadrer un transfert international de données et comment le mettre en œuvre

Comment utiliser des règles internes d'entreprise (« binding corporate rules » ou « BCR ») ?

Dans les cas spécifiques de traitements mis en œuvre pour le compte de l'Etat tel que prévu aux articles 26-I et 26-II *(traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales)*, une autorisation de transfert des données concernées ne peut être accordée que par décret en Conseil d'État pris après avis motivé et publié de la CNIL.

- **Une série d'exceptions d'interprétation stricte : consentement de la personne ou transfert nécessaire à certaines conditions**

Les alinéas 1 à 7 de l'article 69 de la loi du 6 janvier 1978 prévoient qu'un responsable de traitement peut cependant transférer des données à caractère personnel vers un État n'accordant pas une protection adéquate si :

- la personne à laquelle se rapportent les données a consenti expressément à leur transfert
- **ou** si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures pré-contractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

Attention : Ces exceptions n'ont vocation à s'appliquer que dans des cas limités.

Sur le champ d'application de ces exceptions, se reporter à la question 9 :

Dans quelles conditions utiliser les exceptions des alinéas 1 à 7 de l'article 69 de la loi (consentement de la personne ou transfert nécessaire à certaines conditions)?

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00



Quand considère-t-on qu'il y a un transfert de données à caractère personnel ?

La notion de transfert n'est définie ni par la directive 95/46 ni par la loi du 6 janvier 1978 mais doit s'entendre au sens large.

Constitue ainsi un transfert de données vers un pays tiers **toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, copie ou déplacement de ces données d'un support à un autre, quel que soit le type de ce support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire**.

Un traitement est lui-même défini par la loi comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

Les exemples suivants illustrent quelques situations dans lesquelles se produiront des transferts internationaux de données aura lieu en application de la loi:

- centralisation intra-groupe de la base de données de gestion des commandes et de la comptabilité clients,
- centralisation intra-groupe de la base de données de gestion des ressources humaines d'un groupe multinational ;
- transfert vers un prestataire aux fins de saisie informatique de dossiers manuels,
- recours à un centre d'appel étranger et transfert du fichier correspondant pour démarchage ou qualification ;
- hébergement et exploitation de plateformes informatiques ;
- systèmes internationaux de maintenance informatique ;
- etc.

Ne constituent pas des transferts de données à caractère personnel devant être encadrés comme tels au sens de la loi :

- **l'inscription par une personne de données à caractère personnel concernant des tiers sur une page Internet**, bien que cette inscription rende ces données accessibles à des personnes se trouvant dans des pays tiers (jurisprudence de la Cour Européenne de Justice : arrêt Lindqvist du 6 novembre 2003)
- **les cas dans lesquels une personne communique elle-même des données la concernant à une entité établie dans un pays tiers (notamment via un site Web ou un Intranet).**

  Cependant : si une entité établie en France a mis en place un dispositif impliquant que les personnes concernées communiquent elles-mêmes leurs données à un prestataire aux fins d'un traitement dont les finalités et les moyens ont été déterminés par lui, cette entité française sera considérée comme responsable de ce traitement effectué par le destinataire. A ce titre, la communication de leurs données par les personnes devra être considérée comme

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00



les moyens d'un transfert de données que les parties impliquées devront encadrer de manière adéquate.

Exemple : les bénéficiaires d'un programme d'attribution de stock options communiquent au prestataire financier choisi par leur employeur des données les concernant qui seront nécessaires à la liquidation de leurs options. Dans la mesure où l'employeur a mis en place ce programme et a choisi ce prestataire, il restera responsable des traitements effectués par le prestataire, y compris sur les données communiquées ultérieurement par les employés. A ce titre, il devra déclarer le transfert et obtenir une autorisation de transfert par la CNIL.

Attention :
Il convient toujours de s'interroger sur les questions de droit national applicable que peuvent soulever des situations dans lesquelles une communication de données ne peut être considérée comme un transfert au sens de la loi : le responsable de traitement destinataire des données peut parfois être tenu d'appliquer directement la loi du 6 janvier 1978 même s'il est établi hors de l'Union européenne (article 5 de la loi).

8 rue Vivienne –CS 30223 - 75083 Paris Cedex 02 - Tél. : 01 53 73 22 22 - Fax : 01 53 73 22 00



Pourquoi encadrer les transferts de données à caractère personnel vers des pays n'appartenant pas à l'Union européenne ?

Les dispositions de la loi du 6 janvier 1978 et de la directive 95/46/CE du 24 octobre 1995 en matière de transferts de données vers des pays n'appartenant pas à l'Union européenne visent à éviter un contournement de la protection accordée dans ces pays par un transfert.

Elles visent ainsi à assurer que les personnes bénéficiant d'une protection au regard du traitement de leurs données en France continuent à en bénéficier lorsque leurs données quittent le territoire français pour faire l'objet d'un traitement hors de l'Union européenne.

Les pays appartenant à l'Union européenne ont tous transposé dans leur droit national la directive 95/46/CE du 24 octobre 1995 et accorde, de ce fait, une protection équivalente à celle accordée par la loi française du 6 janvier 1978. Les transferts envisagés vers des pays membres de l'Union européenne sont donc libres, dès lors qu'ils obéissent à l'ensemble des autres dispositions de la loi du 6 janvier 1978.

Le même régime s'applique aux pays de l'Espace économique européen (Liechtenstein, Norvège, Islande).

Attention:

les règles relatives aux transferts internationaux de données n'encadrent que les transferts de données à caractère personnel qui quittent le territoire français à destination de pays n'appartenant pas à l'Union européenne.

Elle n'ont pas vocation à encadrer les transferts issus de pays tiers à destination du territoire français.

En revanche, elles s'appliqueront si les données importées en France quittent de nouveau le territoire français à destination d'un pays n'appartenant pas à l'Union européenne.



Quelles sont les autres règles à respecter ?

Un transfert de données vers l’étranger, comme une communication de données à un tiers sur le territoire français, constitue un traitement de données à caractère personnel. Il est soumis à ce titre à l’ensemble des dispositions de la loi du 6 janvier 1978.

L’article 2 de la loi nouvelle définit en effet comme un tel traitement « toute opération ou tout ensemble d’opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment (…) la communication par transmission, diffusion ou toute autre forme de mise à disposition » de ces données. Cette définition, qui reprend intégralement celle de l’article 2 de la directive 95/46/CE du 24 octobre 1995, est délibérément large et recouvre les transferts internationaux.

Les responsables de traitement établis en France doivent donc s’assurer de ce que le transfert qu’ils envisagent d’effectuer répondent à l’ensemble des règles de la loi du 6 janvier 1978, et non seulement à celles des dispositions de la loi qui traitent des transferts vers des pays n’appartenant pas à l’Union européenne.

Il en résulte en particulier que :

- **Le traitement doit avoir régulièrement fait l’objet des formalités préalables requises par la loi** : la CNIL ne saurait autoriser un transfert de données dès lors que le traitement original dont les données sont issues n’aurait pas été déclaré ou autorisé.
- **Tout transfert de données vers l’étranger doit avoir une finalité déterminée, explicite et légitime** : le responsable de traitement établi en France doit pouvoir expliquer pourquoi le transfert a lieu et s’être assuré que ces raisons sont compatibles avec les exigences de la loi française.
- **Les données transférées ne doivent pas être traitées ultérieurement de manière incompatible avec cette finalité :** le responsable de traitement doit pouvoir établir que la raison pour laquelle les données sont transférées est compatible avec les raisons pour lesquelles les données ont été initialement collectées.
- **Les données transférées doivent être adéquates, pertinentes et non excessives** au regard de la ou des finalités pour lesquelles elles sont transférées (article 6 de la loi nouvelle).

A titre d’exemple, la CNIL constate fréquemment que des sociétés multinationales envisagent d’opérer des transferts concernant **l’intégralité du personnel** de sociétés françaises dans le cadre de la centralisation des bases de données « ressources humaines » de leur groupe.

Il est parfois prévu que ces transferts portent sur **la totalité ou la quasi-totalité des informations nominatives relatives aux salariés**, en particulier leur NIR, des données touchant à des aspects de leur vie privée ou à des données qui paraissent *a priori* ne devoir relever que d’une gestion locale.

Ces dossiers peuvent poser des problèmes de légitimité du transfert et de pertinence des données au regard de la finalité du transfert. En effet, bien que la CNIL ne remette pas en cause le mode de fonctionnement de groupes internationaux, l’existence de liens capitalistiques entre sociétés ne saurait en elle-même justifier une centralisation généralisée des données collectées par les sociétés d’un groupe auprès, en particulier, de la holding de celui-ci.

Un transfert de données ne répondant pas à ces conditions serait illégal et pourrait, à ce titre, engager la responsabilité pénale du responsable de traitement.



Attention :

cet exercice d'analyse de la légitimité du transfert doit être accompli quelque soit la base juridique sur laquelle le transfert est envisagé (pays accordant un niveau de protection adéquate, contrat, « règles internes », exceptions de l'article 69 al.1à 8).



Quelles sont les sanctions pénales applicables ?

Différentes dispositions du Code pénal sont susceptibles de sanctionner des manquements aux règles sur les transferts internationaux de données.

En particulier, les dispositions relatives au non-respect des formalités préalables prévues par la loi (déclaration ou autorisation, y compris sur les transferts de données) sont applicables (Art. 226-16 et 226-16 A):

> Art. 226-16 : « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

> Art. 226-16 A : « le fait de ne pas respecter, y compris par négligence, les normes simplifiées ou d'exonération établies à cet effet par la Commission nationale de l'informatique et des libertés est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

En outre, l'Art. 226-22-1 du Code pénal dispose :

> « Le fait, hors les cas prévus par la loi, de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un État n'appartenant pas à la Communauté européenne en violation des mesures prises par la Commission des Communautés européennes ou par la Commission nationale de l'informatique et des libertés mentionnées à l'article 70 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »



Le destinataire est-il responsable de traitement ou sous-traitant ?

La qualification de responsable de traitement ou de sous-traitant sera essentielle pour déterminer la manière dont encadrer les transferts internationaux de données entre les parties.

Le critère essentiel de distinction entre la qualification de « responsable de traitement » et celle de « sous-traitant » est celui de **l'autonomie de l'importateur des données quant à l'usage qu'il pourra faire des données qui lui sont transférées**.

- ### Définition du responsable de traitement

Un responsable de traitement est défini dans la loi comme « la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et les moyens du traitement ». **Un responsable de traitement se caractérise donc par son autonomie dans la mise en place et la gestion d'un traitement**.

Cette autonomie peut n'être que relative.

Ainsi, même dans l'hypothèse où la maison mère d'un groupe multinational détermine seule les finalités et les moyens d'un traitement dont elle impose la mise en œuvre à ses filiales, celles-ci ne peuvent être considérées comme sous-traitants pour la partie du traitement qu'elles réalisent pour leur propre compte. Elles seront considérées comme responsables de traitement et les transferts qu'elles réaliseront ultérieurement vers leur maison mère devront être considérés comme des transferts de données de responsable de traitement à responsable de traitement, soumis aux règles des articles 68 et suivants de la loi du 6 janvier 1978.

Cette interprétation se comprend notamment au regard des dispositions de l'article 4-1-a de la directive 95/46/CE du 24 octobre 1995. Cet article dispose que chacun des établissements d'un même responsable de traitement, quand ils sont situés dans différents États membres, est individuellement tenu par les dispositions de la loi nationale de protection des données personnelles qui lui sera applicable.

Exemple :

La holding d'un groupe multinational impose à ses filiales la mise en place d'un système centralisé de gestion de la paie et de gestion des ressources humaines, dont elle détermine les moyens informatiques. Les filiales du groupe, bien qu'elles n'aient pas décidé de la mise en place de ce système centralisé, et malgré leur absence d'autonomie sur la détermination des moyens du traitement, restent responsables de traitement pour les traitements « gestion de la paie » et « gestion des ressources humaines » qu'elles effectuent pour leur propre compte en France.

- ### Définition du sous-traitant

A l'inverse, **un sous-traitant** aura pour mission d'exécuter des tâches précises sur les instructions et sous la seule et unique responsabilité du responsable de traitement, importateur des données (art. 35 de la loi : « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi »).

A titre d'exemple, seront considérés comme sous-traitants :

- une société offrant des prestations d'hébergement informatique des applications utilisées par le responsable de traitement ;
- une société effectuant des opérations de saisie informatique d'informations communiquées par le responsable de traitement sous forme de dossiers papier ;
- une société gérant un centre d'appels pour le compte du responsable de traitement (service clients notamment) ;
- un prestataire financier gérant un programme de stock options pour le compte d'une société ayant attribué des options à certaines catégories de son personnel

A noter :

la loi du 6 janvier 1978 contient désormais des dispositions spécifiques relatives au recours à des sous-traitants. Ces dispositions devront être satisfaites que ce sous-traitant soit établi ou non sur le territoire de l'Union européenne :

L'article 35 3° de la loi prévoit que « le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en oeuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures ».

L'article 35 4° prévoit que « le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. »



Les personnes concernées ont-elles été informées du transfert de leurs données à l'étranger ?

Les personnes dont les données sont susceptibles d'être transférées doivent être informées de l'existence de ce transfert (article 32 I 7° de la loi du 6 janvier 1978 modifiée).

Cette information doit être suffisamment détaillée, et indiquer notamment la finalité du transfert, le pays d'établissement du destinataire des données (y compris le fait que ce pays n'accorde pas une protection adéquate au sens de la directive européenne 95/46 du 24 octobre 1995), le ou les catégories de destinataires des données et, le cas échéant, de la nature de la protection assurée aux données transférées (contrat, règles internes, Safe Harbor, etc.).

Dans les cas où, comme le prévoit le second alinéa de l'article 32-III de la loi, l'information des personnes auprès desquelles les données n'auraient pas été recueillies se révèlerait impossible ou exigerait des efforts disproportionnés par rapport à l'intérêt de la démarche, il revient au responsable de traitement de prouver cette impossibilité ou ce caractère disproportionné.

L'article L. 432-2-1 du Code du travail prévoit également que le comité d'entreprise doit être informé sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci : le transfert de données relatives au personnel doit également faire l'objet d'une telle **information collective**.

Un second décret d'application de la loi du 6 janvier 1978 modifiée précisera les dispositions de l'article 32 de la loi du 6 janvier 1978.



« Pays équivalent », « pays adéquat », « pays non adéquat » : quel est le statut des législations de protection des données personnelles dans le monde ?

- ## Pays de l'Union européenne

Les 27 pays de l'Union européenne ont adopté des législations de protection des données personnelles transposant dans leur droit national la directive 95/46/CE du 24 octobre 1995.

Ces législations doivent dès lors être considérées comme équivalentes à la loi française. Les transferts vers ces pays sont libres et ne doivent pas faire l'objet de formalités spécifiques auprès de la CNIL.

- ## Pays de l'Espace Economique Européen : Islande, Liechtenstein et Norvège

L'Islande, le Liechtenstein et la Norvège, membre de l'Association Européenne de Libre Echange (AELE), ont transposé la directive 95/46 dans leur droit national en application des obligations imposées à cet égard par l'accord sur l'Espace économique européen (EEE). En effet, en vertu de cet accord, ces trois pays sont tenus de transposer l'acquis communautaire dans leur droit national dans les domaines couverts par l'EEE. A ce titre, l'Islande et la Norvège ont adopté des lois de transposition de la directive 95/46 en 2000, et le Liechtenstein en 2002.

Dès lors, les législations de ces trois pays doivent être considérées comme équivalentes à celles des pays de l'Union européenne et les transferts vers ces pays ne doivent pas faire l'objet de formalités spécifiques auprès de la CNIL.

La Suisse, quatrième pays membre de l'AELE, ne fait pas partie de l'EEE. La législation fédérale suisse ne peut donc être considérée comme « équivalente » à la loi française, mais elle a cependant fait l'objet d'une décision de reconnaissance d'adéquation par la Commission européenne (voir *infra*.)

- ## Pays ayant fait l'objet d'une reconnaissance de protection adéquate par la Commission européenne

Le Conseil et le Parlement européen ont donné le pouvoir à la Commission de décider sur base de l'article 25(6) de la directive 95/46/CE qu'un pays tiers offre un niveau de protection adéquat en raison de sa législation interne ou des engagements pris au niveau international.

L'effet de ces décisions d'adéquation est que les transferts de données vers des destinataires établis dans ces pays ne requièrent pas d'encadrement particulier (contrat, règles internes, etc.).

Les transferts vers ces pays ne doivent pas faire l'objet de formalités spécifiques auprès de la CNIL, mais la mention de l'existence de ce transfert est nécessaire dans le cadre des formalités préalables applicables au traitement principal.

A l'heure actuelle, la Commission européenne a adopté de telles décisions d'adéquation pour les pays suivants :

- **L' Argentine** - Décision de la Commission C(2003)1731 du 30 juin 2003



- **Le Canada** - Décision de la Commission 2002/2/EC du 20 décembre 2001

  La décision d'adéquation du 20 décembre 2001 ne porte que sur la loi canadienne sur la protection des renseignements personnels et les documents électroniques (LRPDE, « PIPEDA », en anglais) du 13 avril 2000.

  Cette loi s'applique aux organisations du secteur privé qui collectent, utilisent ou communiquent des données personnelles dans le cadre d'activités commerciales, dans la mesure où ces entreprises relèvent du champ d'application de la loi fédérale.

  Ainsi, seuls les transferts de responsables de traitement établis dans l'Union européenne vers des sociétés couvertes par cette législation sont libres et n'ont pas besoin de faire l'objet de formalités préalables auprès de la CNIL.

  Attention : Les transferts vers ces sociétés qui ne concernent que des cas de sous-traitance ne rentrent pas dans le champ d'application de la décision ; ces transferts doivent être encadrés par contrat.

  La Commission européenne a établi une liste des « questions fréquemment posées » (« FAQ ») sur le champ d'application de cette décision. Cette liste est disponible sur le site de la Commission européenne en cliquant ici : FAQ sur l'adéquation de la loi canadienne LPRPDE

- **Guernesey -** Décision de la Commission du 21 novembre 2003
- **L' Ile de Man -** Décision de la Commission 2004/411/CE du 28 avril 2004
- **Jersey –** Décision de la Commission 2008/393/CE du 8 Mai 2008
- **La Suisse -** Décision de la Commission 2000/518/EC du 26 juillet 2000
- **Le cas particuliers des entreprises américaines adhérentes au Safe Harbor :** Décision de la Commission 2000/520/EC du 26 juillet 2000 –

  Se reporter à Qu'est-ce que le Safe Harbor ?

Voir :

Sur le site de la Commission européenne : *Décisions de la Commission européenne relative à la constatation du caractère adéquat de la protection des données dans les pays tiers*.

Le document établi par la CNIL : *Panorama des législations de protection des données personnelles dans le monde* (dates et intitulés des législations nationales ; coordonnées des autorités de contrôle)

La *carte interactive* établie par la CNIL qui vous aide à déterminer le statut de protection dans le pays destinataire



Qu'est-ce que le Safe Harbor ?

Le cas particulier du dispositif dit de « Safe Harbor », ou « Sphère de sécurité », repose sur une démarche volontaire d'entreprises établies aux Etats-Unis qui s'auto-certifient comme adhérant à une série de principes de protection des données personnelles et de protection de la vie privée, publiés par le ministère du commerce des États-Unis.

Ces principes, négociés entre les autorités américaines et la Commission européenne, sont essentiellement basés sur ceux de la Directive 95/46 du 24 octobre 1995 :

- information des personnes,
- possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes,
- consentement explicite pour les données sensibles,
- droit d'accès,
- sécurité,
- etc.

La Commission européenne a adopté le 26 juillet 2000 une décision d'adéquation qui reconnaît que ces principes de la « Sphère de sécurité » assurent une protection adéquate pour les besoins des transferts de données à caractère personnel depuis l'Union européenne. Les transferts émis à partir de l'Union européenne vers une entreprise ayant adhéré au Safe Harbor ne doivent dès lors faire l'objet d'aucune formalité spécifique (conclusion de contrat, de règles internes, etc.).

Attention : le champ d'application du mécanisme de « Safe Harbor » est restreint :

- à l'heure actuelle, seules peuvent adhérer au Safe Harbor les sociétés relevant de la compétence de la Federal Trade Commission ou du US Department of Transportation ;

- les sociétés adhérentes au Safe Harbor doivent effectuer des démarches complémentaires afin que les données concernant le personnel des sociétés exportatrices soient couvertes par ce dispositif.

Le US Department of Commerce fournit sur son site l'ensemble des informations pratiques relatives au dispositif du Safe Harbor (liste des entreprises adhérentes, principes de protection, comment devenir adhérent, etc.) : http://www.export.gov/safeharbor

Les responsables de traitement établis en France dont les formalités préalables auprès de la CNIL mentionnent l'existence d'un transfert de données vers une société adhérente au « Safe Harbor » devront fournir à la Commission les extraits pertinents de la « Safe Harbor List », disponible sur ce site. Cette liste permet d'avoir accès aux détails de l'auto-certification de la société adhérente.

La décision de la Commission, y compris une liste des « questions fréquemment posées » (« FAQ ») sur le dispositif de Safe Harbor (annexe 2 de la décision) est disponible sur le site de la Commission européenne et peut être téléchargée en cliquant ici :

Décision de la Commission européenne sur le Safe Harbor



Quel contrat utiliser pour encadrer un transfert international de données et comment le mettre en œuvre ?

- ## Que prévoit la loi ?

La loi prévoit qu'un responsable de traitement envisageant de transférer des données à caractère personnel vers un destinataire établi dans un pays n'accordant pas une protection adéquate pourra se reposer, pour ce faire, sur des « clauses contractuelles ».

La CNIL est l'autorité européenne qui a, la première, eu recours à cette solution contractuelle. Cette solution a été reprise dans la directive 95/46/CE et figure désormais expressément dans la loi du 6 janvier 1978.

- ## Quelle est la qualification applicable : transfert de responsable de traitement à responsable de traitement, ou transfert de responsable de traitement à sous-traitant ?

Cet exercice de qualification préalable conditionnera le type de contrat que les parties devront conclure entre elles.

Sur ce point, se reporter à :
Le destinataire est-il responsable de traitement ou sous-traitant ?

- ## Qu'est-ce que les clauses contractuelles types de la Commission européenne ?

Afin de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert, la Commission européenne a émis des clauses contractuelles types pouvant être utilisées par les responsables de traitement à l'origine du transfert de données et les destinataires de ces données pour encadrer ce transfert.

- Pour les **transferts de responsables de traitement à sous-traitants** : la Commission européenne n'a émis qu'une seule décision, le 27 décembre 2001.
- Pour **les transferts de responsables de traitement à responsables de traitement**, la Commission européenne a émis deux décisions, la première le 15 juin 2001, la seconde le 7 janvier 2005.

Les ensembles de clauses types émises par ces deux décisions concernant les transferts de responsable de traitement à responsable de traitement constituent une **alternative.**

Le second ensemble de clauses contractuelles types résulte des négociations d'une coalition d'associations d'entreprises, sous la direction de la Chambre de commerce internationale, avec la Commission et le comité des autorités européennes chargées de la protection des données (le groupe dit « de l'article 29 »).

Les entreprises estiment que certaines des nouvelles clauses, comme celles relatives aux contentieux, à la répartition des responsabilités ou aux exigences d'audit, sont plus favorables aux entreprises. Elles fournissent cependant un niveau de protection des données similaire à celui offert par les clauses de 2001 et, pour empêcher les abus, les autorités chargées de la protection des données sont investies de davantage de pouvoirs pour intervenir et imposer des sanctions, le cas échéant. La mise en œuvre de ces nouvelles clauses sera revue en 2008.



- **Pourquoi utiliser les clauses contractuelles types de la Commission européenne ?**

Ni le texte de la directive 95/46 ni la loi française n'interdisent d'avoir recours à d'autres clauses que les clauses contractuelles types adoptées par la Commission européenne. Toutefois, la CNIL promeut l'utilisation des clauses contractuelles types, essentiellement pour les avantages qu'elles représentent en terme de sécurité juridique :

- D'une part, dès lors que le transfert peut être considéré comme légitime et que les clauses contractuelles types sont mises en œuvre de manière satisfaisante (clauses reprises *in extenso*, annexes complètes, etc.), les autorités européennes de protection des données personnelles, dont la CNIL, sont tenues de considérer que le transfert a lieu dans des conditions satisfaisantes au regard des droits des personnes dont les données sont transférées (article 26(4) de la directive) ; la sécurité juridique en découlant est donc maximum.

- D'autre part, les autorités européennes de protection des données personnelles sont tenues d'informer la Commission européenne et les autres Etats membres des autorisations de transfert qu'elles accordent aux responsables de traitement. Au cas où la Commission ou l'un de ces Etats manifesterait son désaccord avec cette autorisation, la Commission européenne sera seule compétente pour décider de la solution finale à appliquer (article 26(3) de la directive). L'utilisation des clauses contractuelles types limite donc les incertitudes et les risques de blocage induits par cette procédure.

- En tout état de cause, un contrat autre qu'un contrat basé sur les clauses contractuelles types devrait reprendre au moins l'essentiel, si ce n'est toutes les garanties prévues par ces clauses types, celles-ci constituant désormais une référence. L'intérêt de la rédaction d'un contrat alternatif est donc quasi inexistant.

- **Peut-on soumettre à la CNIL un contrat qui ne soit pas basé sur les clauses contractuelles types ?**

Ni la loi ni la directive n'interdisent d'avoir recours à un contrat qui ne soit pas basé sur les clauses contractuelles types pour encadrer des transferts de données hors de l'Union européenne.

Toutefois, dans le cadre de l'autorisation de transfert qu'elle délivre, la CNIL doit s'assurer que ce contrat accorde des « garanties suffisantes » ou un « niveau de protection suffisant », au sens de la directive et de la loi. La CNIL appréciera le niveau de ces garanties par référence au niveau de protection résultant des clauses contractuelles types émises par la Commission européenne.

Afin de faciliter cette analyse et ainsi le traitement de leur dossier, les responsables de traitement peuvent accompagner leurs projets de contrat alternatifs avec un tableau de correspondance entre les clauses de ce contrat et les clauses contractuelles types de la Commission européenne.

A cet effet, la CNIL met à la disposition des responsables de traitement un tableau de concordance entre de tels contrats et les clauses contractuelles types du 15 juin 2001. Ce tableau est disponible en annexe à ce guide pratique.

- **La CNIL a-t-elle une préférence entre les clauses contractuelles types du 15 juin 2001 et du 7 janvier 2005 pour les transferts de responsable de traitement à responsable de traitement ?**

Non. Les responsables de traitement sont libres d'avoir recours à l'un ou l'autre ensemble de clauses que la CNIL tient pour strictement équivalentes.

- **Peut-on modifier les clauses contractuelles types ?**

Les avantages découlant de l'utilisation des clauses contractuelles types de la Commission européenne qui ont été rappelés plus haut sont liés à la condition d'une **reprise intégrale du texte des clauses types**.

Toute modification apportée aux clauses, dans la mesure où elle serait susceptible de modifier l'équilibre de la protection qu'elles accordent, délierait la CNIL de son obligation de considérer que le transfert a lieu dans des conditions satisfaisantes au regard des droits des personnes dont les données sont transférées.

Cependant, **des aménagements sont envisageables quand ils ne modifient pas le contenu de la protection accordée par ces clauses**. Il appartient au responsable de traitement qui communique ce contrat à la CNIL dans le cadre de son pouvoir d'autorisation préalable des transferts (art. 69 al. 8) d'indiquer la localisation et le contenu de ces modifications, afin de permettre à la Commission d'en apprécier les conséquences.

Il est également possible que les clauses contractuelles types soient incluses dans un **contrat multipartite**, quand une telle configuration contractuelle est nécessaire pour être fidèle à la réalité du transfert envisagé.

Par exemple, dans la situation où un responsable de traitement aurait recours à un sous-traitant établi en France, mais qui aurait lui-même recours à un sous-traitant établi dans un pays tiers, la configuration contractuelle retenue devra nécessairement inclure le responsable de traitement, le sous-traitant et son propre sous-traitant, afin d'être conforme à la réalité des transferts envisagés, en considérant le responsable de traitement et son sous-traitant comme exportateurs des données, d'une part, et la société sous-traitante établie dans un pays tiers comme importatrice, d'autre part.

- **Comment utiliser les clauses types « responsable de traitement à responsable de traitement » ?**

Les clauses contractuelles types (responsable de traitement à responsable de traitement) sont structurées en quatre parties, les deux dernières étant alternatives.

Sur le corps du contrat (les « clauses contractuelles types » proprement dites)

Cette partie du contrat, que les parties ne peuvent modifier, précise essentiellement les obligations générales des deux parties (ex : leurs obligations d'information envers les personnes ; le traitement des demandes de renseignement de la part de celles-ci; l'audit des moyens de traitement du destinataire, etc.), leur responsabilité réciproque, leur responsabilité envers la personne dont les données sont transférées, et la mise en place de procédures de médiation.

Une clause particulière est la clause dite de « tiers bénéficiaire » (clause 3) : cette « stipulation pour autrui » consiste à permettre aux personnes dont les données sont transférées de se prévaloir des termes du contrat, quand bien même elles n'y sont pas formellement parties, dans les cas où elles

subiraient un dommage du fait du non-respect par l'une des parties de ses obligations. Dans ces cas, cette clause permet notamment à ces « tiers bénéficiaires » d'invoquer les termes du contrat pour demander l'exécution par la partie en question de ses obligations. Tant la Commission européenne que les autorités européennes de protection des données s'accordent sur le caractère fondamental de cette clause, qui doit dès lors toujours être présente dans les contrats de transfert.

Attention :

les clauses contractuelles types imposent d'effectuer un choix à la clause 5(b), relative aux obligations du destinataire des données, déterminant les principes de protection des données que le destinataire des données s'engage à respecter contractuellement.

Les parties doivent effectuer un choix entre **trois possibilités**, qui consistent pour le destinataire des données à s'engager à respecter :

- soit aux dispositions pertinentes du droit national de l'exportateur (c'est à dire les obligations imposées aux responsables de traitement par la loi du 6 janvier 1978, en ce qui concerne les transferts de données à partir de la France) ;

- soit une liste de principes de protection détaillées à l'annexe 2 des clauses contractuelles types ;

- soit, pour des destinataires potentiels établis aux USA, la liste des principes du Safe Harbor, complétés par la liste des principes listés à l'annexe 3 du contrat, dans des cas où le destinataire ne relève pas du champ d'application du Safe Harbor.

En pratique, l'option la plus fréquemment retenue consiste à choisir de respecter la liste exhaustive des principes établie par l'annexe 2 des clauses contractuelles types. Toutefois, les cas ne sont pas rares dans lesquels les parties omettent d'effectuer ce choix et reprennent ainsi l'intégralité des clauses et des annexes sans les compléter : la formulation des obligations de l'importateur en devient imprécise et ambiguë.

Le paragraphe 3 de la clause 6, relative à la répartition de la responsabilité des parties, est optionnel : les parties restent en effet libres de fixer entre elles la manière dont elles souhaitent répartir les dommages-intérêts potentiels résultant d'une action judiciaire intentée à leur encontre par une personne qui aurait subi un dommage du fait d'un manquement à une de leurs obligations contractuelles.

Annexe 1 des clauses types (annexe précisant le détail du transfert)

Les clauses contractuelles types exigent que soient fournies dans cette annexe, à tout le moins, les informations suivantes (les autorités nationales de contrôle étant libres de demander plus d'informations si elles l'estiment nécessaire) :

- identification du responsable de traitement établi en France (« exportateur ») et du, ou des destinataire(s) (« importateur(s) ») ;
- Catégories de personnes concernées par les données transférées ;
- Finalités du transfert ;

- Catégories de données transférées ;
- Données sensibles (le cas échéant) ;
- Destinataires des données ;
- Durées de conservation.

La CNIL préconise une rédaction spécifique quand le contrat porte sur plusieurs types de transferts : il convient alors de fournir les détails de chaque transfert dans différentes annexes, chacune d'entre elles correspondant à une finalité de transfert (ex : gestion de la clientèle / administration d'un programme de stock options / gestion de la paie, etc.). Cette solution permet de distinguer clairement quelles circonstances s'appliquent à quel transfert, et évite ainsi des confusions quant à la justification et à la portée de chacun d'entre eux.

Il conviendra de supprimer le paragraphe relatif aux données sensibles si celles-ci ne font pas l'objet d'un transfert, afin d'éviter tout risque de confusion.

- ## Comment mettre en œuvre les clauses contractuelles types « responsable de traitement à sous-traitant » ?

Dans l'analyse des transferts effectués sur la base des clauses contractuelles types du 27 décembre 2001, la CNIL s'attache particulièrement à la rédaction de l'annexe décrivant les mesures de sécurité mises en œuvre par le sous-traitant.

Cette annexe doit offrir une description générale, mais toutefois suffisamment précise, des mesures de sécurité mises en œuvre, qu'elles soient d'ordre physique (sécurité des locaux) et logique (sécurité du système). Ces mesures de sécurité doivent être à jour compte tenu de l'état de la technique.



Comment utiliser des règles internes d'entreprise (« binding corporate rules » ou « BCR ») pour encadrer des transferts ?

• A quoi servent des « règles internes »?

La loi du 6 janvier 1978 modifiée prévoit expressément qu'il peut être fait recours à des « règles internes » pour encadrer des transferts internationaux de données (art. 69 al. 8). Par « règles internes », il est entendu un **ensemble de règles relatives à la protection des données personnelles élaborées par l'organisme du responsable de traitement, le plus souvent une société multinationale, dont le respect est obligatoire pour chacune des entités membres du groupe**.

En pratique, cette option d'encadrement des transferts internationaux de données est destinée à satisfaire les besoins particuliers des sociétés multinationales au sein desquels les transferts peuvent être importants et d'une grande variété.

La vocation de telles règles internes est d'offrir une **norme interne de référence en matière de protection des données personnelles pour l'ensemble des membres du groupe**. Emises par la direction du groupe, elles contribuent à uniformiser les pratiques et, ce faisant, à prévenir les risques inhérents aux traitements de données personnelles, en particulier au sein des sociétés membres du groupe établies dans des pays ne disposant pas de législation de protection des données personnelles.

C'est au regard de ces caractéristiques que de telles règles internes sont susceptibles d'assurer que « le traitement garantit un niveau de protection suffisant au regard de la vie privée et des droits fondamentaux des personnes », au sens de l'article 69 al. 8 de la loi.

Ainsi, elles peuvent constituer une **alternative à la solution contractuelle** pour encadrer des transferts de données vers des membres de l'organisation établis dans des pays n'appartenant pas à l'Union européenne.

Les règles internes constituent pour les groupes un moyen souvent plus flexible que les contrats d'encadrer les communications de données personnelles en leur sein. En effet, de telles règles, adoptées de manière unilatérale par les plus hautes instances décisionnelles du groupe en la matière, évitent de conclure autant de contrats qu'il existe de transferts en leur sein (ce qui impliquerait que, chaque société pouvant être originaire ou destinataire de données, elle ait à conclure un contrat avec chacune des autres entités du groupe qui se retrouveraient dans la même situation).

• Comment établir des règles internes ?

Le groupe de l'article 29 a adopté un document de travail sur ces questions, dit document WP 74. Ce document détermine les conditions générales dans lesquelles de telles règles internes doivent être élaborées et les grandes lignes du contenu de ces règles.

Le contenu de ce document a été ultérieurement précisé par un autre document du groupe de l'article 29, dite « model checklist » (document WP 108) (disponible en anglais seulement à l'heure actuelle).



Les éléments essentiels que doivent pouvoir établir les responsables de traitement souhaitant faire valider leurs règles internes dans le cadre d'une autorisation de transfert sont les suivants :

- le caractère contraignant des règles doit être établi (en interne et en externe) ;
- des mesures doivent être prises qui assurent l'application des règles internes en pratique dans l'organisation ;
- les personnes doivent avoir la possibilité de se prévaloir de l'existence de ces règles ;
- les règles internes doivent décrire avec suffisamment de précision les transferts couverts par les règles et les traitements correspondants, afin d'offrir une sorte de « mode d'emploi » de la protection des données personnelles au sein de l'entreprise pour les personnes appelées à en traiter ;
- des garanties doivent être prises pour que les principes de la protection des données personnelles soient appliqués en pratique dans le groupe (information des personnes ; sécurité des données ; droit d'accès ; respect du principe de finalité, etc.).

Il est évident que de telles règles internes ne pourront trouver à s'appliquer que dans la mesure où elles respectent l'ensemble des législations applicables dans chacun des pays dans lesquels les entités du groupe seront appelées à opérer des traitements de données personnelles.

Dès lors, les règles internes ayant vocation à servir de norme générale à toutes les entités d'un groupe multinational, dans quelques pays qu'elles soient établies, **ces règles internes n'auront de sens que dans la mesure où elles s'aligneront sur le plus haut dénominateur commun en matière de protection des données personnelles**.

- **Comment assurer que des règles internes lient effectivement les membres du groupe ?**

Le document WP 74 et la « model checklist » adressent tous deux ces questions de la nature « contraignante » des règles internes. Ce caractère contraignant doit être établi de différentes manières. En particulier :

Les différentes entités du groupe doivent être effectivement tenues d'appliquer ces règles internes

Il ne revient pas à la CNIL de déterminer comment les groupes peuvent assurer que leurs filiales sont effectivement liées par les règles internes. Les responsables de traitement qui sollicitent une autorisation de transfert de la CNIL devront prouver que ce caractère contraignant est effectif à travers l'ensemble du groupe.

Le document du groupe de l'article 29 intitulé « checklist » fournit différents éléments de nature à assurer cette nature contraignante des règles internes entre les différentes entités du groupe (existence de conventions passées entre les entités du groupe ; mise en place de codes de conduite ou de « policies », etc.).

Les salariés de chaque entité du groupe doivent être tenus de respecter ces règles internes

Sont pertinents à cet égard la prévision de **sanctions disciplinaires** en cas de manquement à ces règles, l'inclusion d'**obligations contractuelles** dans le contrat de travail, etc.

- **Que doit-il être prévu au bénéfice des personnes concernées en cas de dommage subi du fait du transfert ?**

Les règles internes doivent prévoir que les personnes dont les données seront transférées sur la base de ces règles pourront obtenir réparation de tout préjudice éventuellement subi par elles du fait de ce transfert, que ce dommage résulte du fait de la société importatrice ou de la société exportatrice.

Le document WP 74 et le document « model checklist » donnent plus de détails sur ce point, en précisant notamment que la personne concernée doit pouvoir se retourner vers la société la plus proche d'elle en cas de besoin (en pratique, la société exportatrice avec laquelle la personne est en contact direct).

Les règles internes doivent cependant, afin de prévenir de telles situations impliquant le recours aux juridictions judiciaires, prévoir des procédure de médiation et de règlement amiable des litiges. Ces dispositions spécifiques des règles internes doivent explicitement faire mention de la possibilité, pour la personne concernée, d'avoir recours aux services de l'autorité de contrôle compétente (en France, la CNIL).

- **Quelles sont les mesures qui assureront que les règles seront effectivement appliquées en pratique ?**

Il revient au groupe de prendre des mesures permettant d'être certains que les règles internes sont effectivement appliquées en son sein, en particulier par la mise en place de **procédures d'audits**.

Des **mesures de formation** du personnel doivent être prévues qui donnent à celui-ci la possibilité d'appliquer les règles internes en pratique. D'autres éléments pertinents sont évoqués dans le document « model checklist », tel que l'**implication active du personnel de direction** dans le respect de ces règles.

- **Quel est le niveau de détail requis quant aux transferts couverts par les règles ?**

Le document WP 74 mentionne explicitement le fait que les règles internes doivent fournir un certain niveau de détail quant à la manière dont les données personnelles devront être traitées par les différentes entités au sein du groupe.

En effet, les principes de protection des données personnelles sont susceptibles de ne pas avoir grand sens par en eux-mêmes pour les sociétés et les employés traitant des données personnelles, en particulier dans des pays ne disposant pas de législation dans le domaine de la protection des données personnelles.

Ainsi, les règles internes doivent développer et détailler ces principes en précisant de manière concrète leurs conséquences quant aux opérations de traitement effectuées par l'organisation dans des pays tiers, afin d'être compris et appliqués effectivement au sein de l'organisation.

Ce niveau de détail doit également être suffisant pour permettre aux autorités de contrôle comme la CNIL d'évaluer le caractère adéquat du traitement effectué dans des pays tiers.

Cette partie des règles internes devra en pratique refléter le niveau de détail exigé dans le cadre des formalités préalables à accomplir auprès de la CNIL.

- ### Des transferts vers des entités non membres du groupe peuvent-ils être couverts par les règles internes intra-groupe ?

Non. Il n'est pas possible d'envisager que des transferts ultérieurs vers des sociétés non-membres du groupe (sous-traitants ou responsables de traitement) puissent avoir lieu sur la base des règles internes.

En effet, le caractère contraignant de ces règles ne pourra être établi que vis-à-vis de sociétés membres du groupe. Il ne sera possible de transférer des données à des entités extérieures que sur la base d'un contrat. La CNIL préconise à cet effet d'avoir recours aux clauses contractuelles types émises par la Commission européenne.

- ### Quelle est la procédure à respecter auprès de la CNIL ?

La CNIL n'a pas vocation à autoriser des règles internes en tant que telles.

La Commission n'aura à connaître de telles règles internes que dans la mesure où celles-ci lui seront soumises dans le cadre d'une procédure d'autorisation de transfert de données, en application de l'art. 69 al. 8 de la loi.

Dès lors, ce n'est que dans le cadre d'une telle procédure d'autorisation que la CNIL sera formellement appelée à apprécier si les règles internes seront susceptibles de constituer des garanties suffisantes au regard du transfert envisagé.

Dans ce cadre, il conviendra de fournir à la Commission :

tous les éléments relatifs au traitement principal tels qu'ils sont normalement décrits dans le cadre des formalités préalables applicables ;

dans le cadre de ces formalités, tous les éléments relatifs au transfert proprement dit (annexe 6 du formulaire de déclaration) ;

les différents documents composant les règles internes de l'organisation.

> **Attention :** l'adoption de règles internes n'a pas pour effet de dispenser le responsable de traitement de l'accomplissement des formalités préalables correspondantes auprès de la CNIL.

- ### Est-il possible d'obtenir une autorisation unique de la part de plusieurs autorités européennes de contrôle ?

Ayant vocation à constituer une norme d'application générale au sein d'un groupe multinational, les règles internes devront *a priori* être soumises à l'appréciation de plusieurs autorités de contrôle européennes, dans le cadre de procédures d'autorisation de transfert applicables dans chacun de ces pays.

Afin de faciliter ce processus de soumission de demandes d'autorisations simultanées auprès de différentes autorités de contrôle européennes, le Groupe de l'article 29 a adopté le 14 avril 2005 un document de travail relatif à une « procédure de coopération » (document WP 107) entre ces autorités.

L'objectif de cette procédure est de coordonner les commentaires des autorités compétentes sur les règles internes soumises par un groupe multinational et sur les transferts opérés sur cette base. Cette

procédure est coordonnée par une des autorités de contrôle impliquées dans la procédure, dite « autorité de coordination », qui aura été désignée en vertu de différents critères définis dans le document WP 107.

Cette procédure n'institue en aucun cas un mécanisme de reconnaissance mutuelle qui lierait les autorités y participant à reconnaître des règles internes comme constituant des garanties suffisantes, dès lors que l'autorité de coordination les a reconnues comme telles.

En tout état de cause, la procédure ne pourra aboutir qu'à la délivrance d'autorisations de transfert nationales, en vertu des règles nationales applicables dans chacun des pays dans lesquels le responsable de traitement a déposé une telle demande d'autorisation.

Cependant, cette procédure constitue une garantie de simplification pour les sociétés multinationales qui n'ont dès lors plus à se tourner vers chacune des autorités auprès desquelles elles doivent accomplir des formalités relatives aux transferts : l'autorité de coordination est leur seul point de contact, qui se charge de relayer les commentaires de l'ensemble des autorités impliquées dans la procédure de coordination.



Dans quelles conditions utiliser les exceptions des alinéas 1 à 7 de l'article 69 de la loi (consentement de la personne ou transfert nécessaire à certaines conditions)?

- ## Quelles sont les exceptions prévues par la loi ?

Les alinéas 1 à 7 de l'article 69 de la loi du 6 janvier 1978 prévoient qu'un responsable de traitement peut transférer des données à caractère personnel vers un État n'accordant pas une protection adéquate si :

la personne à laquelle se rapportent les données a consenti expressément à leur transfert

ou si le transfert est nécessaire à l'une des conditions suivantes :

1° A la sauvegarde de la vie de cette personne ;

2° A la sauvegarde de l'intérêt public ;

3° Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;

4° A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;

5° A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures pré-contractuelles prises à la demande de celui-ci ;

6° A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.

- ## Ces exceptions doivent être interprétées strictement

Conformément aux principes généraux du droit français et du droit communautaire, ces dérogations doivent être interprétées strictement car elles impliquent une absence totale de protection dans le pays destinataire pour la personne concernée.

La logique fondamentale des règles françaises et européennes en matière de transferts internationaux de données consiste à assurer aux personnes qu'elles continuent à bénéficier d'une protection même quand leurs données ont été transférées vers un pays tiers.

L'esprit de ces dispositions consacre une priorité implicite du principe de l'exigence d'un niveau de protection adéquate ou de garanties suffisantes mises en œuvre par le destinataire sur les véritables dérogations à ce principe, telles qu'énoncées à l'article 26-1 de la directive (alinéas 1 à 8 de l'article 69 de la loi).

La nécessité d'une interprétation stricte de ces exceptions est conforme à la position du groupe de l'article 29, exprimée notamment dans son document de référence en matière de transferts internationaux de données (document de travail WP 12), ainsi qu'au rapport explicatif du Protocole additionnel à la Convention 108, Article 2.2, a.

Plus récemment, le groupe de l'article 29 a adopté un document de travail spécifiquement dédié à cette question de l'interprétation des dérogations de l'article 26(1) de la directive (document WP114). Ce document affine la première analyse du document WP12 sur ces questions et formule un certain nombre de recommandations.

Le groupe de l'article 29 a conclu dans son document de travail WP 12 que *« ces dérogations, formulées de manière restrictive, ne doivent concerner que des cas dans lesquels les risques pour la personne concernée sont relativement faibles, ou des cas dans lesquels d'autres intérêts (qu'ils soient publics ou propres à la personne concernée elle-même) priment le droit de la personne concernée au respect de sa vie privée »*.

La CNIL recommande ainsi que **le champ d'application des dispositions soit *a priori* limité à des cas exceptionnels dans lesquels il serait réellement inapproprié, voire impossible, que le transfert ait lieu sur la base des dispositions de l'article 69 al.8 (contrat, règles internes).**

Il serait en effet regrettable qu'un responsable de traitement réalise d'importants transferts de données vers des pays tiers sans les encadrer de manière appropriée, alors qu'il aurait les moyens d'accorder une protection aux personnes concernées (contrat de transfert, adoption de règles internes).

La CNIL et le groupe de l'article 29 recommandent en particulier que des transferts répétitifs, massifs ou structurels de données personnelles, dont l'importance ou la régularité justifient qu'ils soient encadrés de manière précise, **fassent l'objet d'un encadrement juridique spécifique et ne reposent donc pas sur ces dérogations**. Le rapporteur du projet de loi de transposition de la directive en seconde lecture devant l'Assemblée nationale s'est attaché à mentionner ce point dans son rapport sur l'article XII du projet de loi relatif aux transferts internationaux de données.

Ainsi, **les responsables de traitement envisageant des transferts de données doivent privilégier des solutions garantissant aux personnes qu'elles continueront à bénéficier des droits et garanties fondamentaux reconnus à l'égard du traitement de leurs données dans l'Union, une fois leurs données transférées** (loi reconnue comme adéquate dans le pays de destination, mise en œuvre de contrats ou de règles d'entreprise contraignantes, etc.), **plutôt que des solutions ne leur garantissant aucune protection.**

En tout état de cause, il revient à la CNIL de s'assurer que ces exceptions sont mises en œuvre de manière satisfaisante. Elles peut intervenir à tout moment auprès des responsables de traitement concernés pour les informer de la nécessité d'encadrer un transfert international de données de manière appropriée plutôt que de se fier aux exceptions de l'article 26, si elle l'estime justifié.

La CNIL a établi des règles relatives à l'interprétation de chacune de ces exceptions, que l'on retrouve également dans le document WP114 du groupe de l'article 29.

- ### Dans quels cas peut-on utiliser le consentement de la personne concernée ?

L'article 69 al.1 prévoit qu'un transfert de données à caractère personnel peut être effectué vers un pays n'accordant pas de protection adéquate à condition que la personne ait « consenti expressément au transfert ».

Pour être valable, dans quelques circonstances qu'il soit donné, ce consentement doit être une manifestation de volonté, libre, spécifique et informée. Telle est en effet la définition du consentement que donne l'article 2(h) de la directive 95/46/CE du 24 octobre 1995.

- **Un consentement, pour être valable, doit être une manifestation positive de volonté**

L'importance que cet acte soit positif exclut donc *de facto* tout système par lequel la personne n'aurait que le droit de s'opposer *a posteriori* au transfert : le consentement de la personne doit réellement conditionner le transfert, lequel ne peut avoir lieu si la personne ne s'est pas spécialement manifestée à cet effet. Tout doute sur le fait que le consentement a bien été donné rendrait la dérogation inapplicable.

Ainsi, les situations dans lesquelles le consentement d'une personne est considéré comme ayant été implicitement donné ne pourront pas être couvertes par cette dérogation.

Par ailleurs, dans son avis relatif à l'interprétation de l'article 13 de la directive « vie privée et communications électroniques », qui introduit un régime harmonisé pour les communications à des fins de prospection directe aux personnes physiques, le groupe de l'article 29 a fourni plusieurs éléments d'interprétation de la notion de « consentement préalable » dans le contexte d'internet, en particulier.

Dans cet avis, le groupe rappelle notamment l'intérêt que présente l'utilisation de cases à cocher aux fins de recueillir le consentement préalable des personnes sur les sites internet. L'utilisation de cases pré-cochées ne saurait satisfaire l'exigence que le consentement soit une manifestation positive de volonté.

- **Le consentement doit être donné librement, et doit pouvoir être retiré librement**

Un consentement donné par une personne qui n'aurait pas la possibilité d'effectuer un véritable choix ou qui aurait été mise devant le fait accompli ne peut être valable.

Ainsi, dans un contexte salarié, c'est-à-dire dans le cadre d'une relation de subordination, le consentement des personnes concernées ne peut *a priori* être considéré comme donné librement.

La doctrine de la CNIL est constante sur ce point. Elle est conforme sur ce point à la position du groupe de l'article 29, telle qu'énoncée dans son avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel, et confirmée dans le document de travail WP114 précité.

L'employé doit avoir la possibilité de refuser de donner son consentement sans préjudice, ou le retirer ultérieurement s'il change d'avis. Or, dans une telle situation de dépendance hiérarchique, le refus ou les réserves d'un salarié exprimées à l'égard du transfert ne sont pas insusceptibles de lui causer un préjudice moral ou matériel qui serait tout à fait contraire à la lettre et à l'esprit des règles françaises et européennes de protection des données personnelles.

A priori donc, les responsables de traitement seraient mal conseillés de se fier uniquement au consentement de leurs employés pour le transfert de leurs données, hormis quelques cas exceptionnels où, si ceux-ci voulaient le retirer ultérieurement, ils n'en subiraient aucune conséquence.

- **Le consentement doit être spécifique**

Pour constituer une base légale valable à un éventuel transfert de données, le consentement donné par la personne doit être spécifiquement donné sur la question du transfert lui-même.

Si la personne est appelée à consentir à plusieurs points, chacun d'eux doit faire l'objet d'une manifestation de volonté distincte, répondant à chacune des conditions prévues dans la directive et dans la loi (consentement libre, spécifique et informé).

Le consentement devant être spécifique, il serait illégal d'obtenir le consentement des personnes *a priori*, par anticipation d'un transfert futur, dont la survenance ou les circonstances précises ne sont pas acquises au jour où le consentement des personnes est requis. A titre d'exemple, une société ne pourra pas, au moment où elle collectera les données de ses clients pour une finalité précise, demander à ceux-ci de consentir par anticipation au transfert de leurs données vers des pays tiers, dans l'éventualité où cette société se ferait hypothétiquement racheter par une société tierce.

- **Le consentement doit être informé**

L'exigence d'information est particulièrement importante. Elle impose au préalable que la personne concernée ait été correctement informée des circonstances spécifiques du transfert (finalité du transfert, identité et coordonnées du ou des destinataires, etc.), en application du principe général de loyauté.

L'information des personnes doit également comprendre le risque spécifique résultant du fait que les données les concernant seront transférées vers un pays n'assurant pas une protection adéquate. Seule cette information permettra à ces personnes de consentir en pleine connaissance de cause ; si elle n'est pas fournie, la dérogation ne s'appliquera pas.

Il s'avère que le consentement est parfois compliqué à obtenir pour des problèmes pratiques, notamment quand le responsable de traitement et les personnes concernées ne sont pas en contact direct. Quelles que puissent être ces difficultés, le responsable de traitement doit pouvoir établir en toutes circonstances qu'il a d'une part obtenu le consentement de chaque personne concernée, et, d'autre part, que ce consentement a été donné sur la base d'informations suffisamment précises incluant l'absence de protection dans les pays tiers.

• Qu'est-ce qu'un transfert nécessaire à la sauvegarde de la vie de la personne concernée ?

Un transfert de données sera de toute évidence nécessaire à la sauvegarde de la vie de la personne concernée quand il sera motivé par l'urgence d'une situation médicale et que les données transférées seront directement nécessaires à l'administration des soins correspondants.

Ainsi, par exemple, il sera possible de transférer sur cette base vers un pays tiers les données relatives à une personne, y compris certaines données sensibles, si cette personne se trouve dans un état d'inconscience rendant nécessaire l'administration de soins urgents et que seul son médecin traitant, établi dans un des pays de l'Union européenne, est à même de fournir ces données.

La motivation du transfert doit se rapporter à l'intérêt individuel de la personne concernée, et un diagnostic vital conditionné par le transfert doit être en cause.

A contrario, il est impossible d'invoquer cette exception pour justifier le transfert de données personnelles à caractère médical à des responsables de traitement établis hors de l'Union européenne, quand ceux-ci n'ont pas pour finalité de traiter le cas précis de la personne concernée, mais, par exemple, d'effectuer des recherches médicales d'ordre général qui ne porteraient leurs fruits que dans les années à venir. Dans ce cas, les transferts devront reposer sur des bases juridiques alternatives.



- **Qu'est-ce qu'un transfert nécessaire à la sauvegarde de l'intérêt public ?**

Conformément à l'interprétation donnée par le groupe de l'article 29 dans son document de travail WP 12, un transfert de données ne peut reposer sur cette dérogation que dans la mesure où ce transfert peut être considéré comme strictement et objectivement nécessaire à la sauvegarde d'un intérêt public important.

Le groupe de l'article 29 s'est déjà prononcé de manière restrictive sur l'interprétation qui doit être faite de la notion de « sauvegarde d'un intérêt public important » dans son avis PNR du 24 octobre 2002. Il avait alors refusé le recours à cette exception pour légitimer le transfert des données des passagers des compagnies aériennes aux autorités américaines qui arguaient d'un tel intérêt public important pour deux raisons : d'une part, le caractère de nécessité du transfert n'était pas établi ; d'autre part, il ne paraissait pas acceptable qu'une décision unilatérale d'un pays tiers, pour des raisons d'intérêt public qui lui sont propres, conduise au transfert régulier et massif de données protégées par la directive.

En effet, il est évident que le législateur européen n'a envisagé ici que ne puissent être pris en compte que des intérêts publics importants qui auraient été déterminés comme tels par la loi nationale applicable aux responsables de traitement établis sur le territoire de l'Union européenne. Toute autre interprétation rendrait aisément possible à une autorité étrangère de contourner le principe d'exigence d'une protection adéquate dans le pays destinataire que pose la directive 95/46.

En revanche, le considérant 58 de la directive 95/46 fait référence à des cas dans lesquels ces échanges internationaux de données pourraient être nécessaires « entre les administrations fiscales ou douanières de différents pays », ou « entre les services compétents en matière de sécurité sociale ». Cette précision, qui semble ne concerner *a priori* que des situations d'investigation de cas particuliers, explicite le fait que cette exception ne pourra être invoquée que dans la mesure où les autorités d'un pays membre de l'Union européenne sont elles-mêmes intéressées au transfert, et non seulement une ou des autorités publiques de pays tiers.

- **Qu'est-ce qu'un transfert nécessaire au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ?**

Comme les dérogations précédentes, la notion de « constatation, sauvegarde ou défense d'un droit en justice » est soumise à interprétation stricte et son application est réservée à des cas particuliers.

Conformément à l'interprétation donnée par le groupe de l'article 29 dans ses documents de travail WP 12 et WP 114, un transfert de données ne peut reposer sur cette dérogation que dans la mesure où une « connexion réelle et substantielle » est établie entre ce transfert et le respect de telles obligations.

Ainsi, l'on peut imaginer que la société mère d'un groupe multinational, établie dans un pays tiers, soit assignée en justice par l'un de ses employés, actuellement en poste auprès d'une filiale française du groupe. Il semble que cette société pourrait légalement requérir de sa filiale qu'elle transfère certaines données relatives à la personne, dans la mesure où celles-ci seraient strictement nécessaires à sa défense, en s'appuyant sur cette dérogation.

En tout état de cause, il est impossible d'avoir recours à cette exception pour justifier le transfert de l'intégralité des dossiers des employés des salariés vers la maison mère du groupe, en arguant de l'éventualité que de telles actions en justice se produisent un jour. Cette exception n'a en effet vocation qu'à être invoquée de manière exceptionnelle.

Cette dérogation ne trouvera par ailleurs à s'appliquer que si les règles de procédure pénale ou civile applicables à ce type de situations internationales le permettent (cf. Conventions de La Haye du 18 mars 1970 et du 25 octobre 1980).

- **Qu'est-ce qu'un transfert intervenant au départ d'un registre public ?**

L'exception prévue par l'article 69 al.1 - 4° concerne les transferts « à la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ».

Cette disposition est une conséquence logique de la nature ouverte et librement consultable des registres auxquelles elle se réfère. En effet, si ces registres sont consultables par tout un chacun sur le territoire national ou par toute personne y ayant un intérêt légitime, il semble *a priori* cohérent de prévoir que cette consultation puisse se faire au profit d'une personne établie dans un pays tiers.

Cette liberté de transfert n'est pas intégrale. Le considérant 58 de la directive 95/46/CE du 24 octobre 1995 prévoit en effet sur ce point que « dans ce cas, un tel transfert ne devrait pas porter sur la totalité des données ni sur des catégories de données contenues dans ce registre ». Il serait en effet non conforme à l'esprit de cette disposition qu'elle puisse servir à vider ces registres de leur contenu, faisant courir le risque, à terme, que ceux-ci puissent être détournés de leur finalité d'origine en étant exploités par des entités établies dans des pays tiers.

Par ailleurs, le même considérant prévoit que « lorsqu'un registre est destiné à être consulté par des personnes qui ont un intérêt légitime, le transfert ne devrait pouvoir être effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires ».

Il conviendra en tout état de cause de se reporter aux dispositions légales ou réglementaires applicables à la consultation du registre concerné afin de vérifier si cette exception pourra trouver à s'appliquer. Ces dispositions légales ou réglementaires définiront en particulier les notions de « destination à l'information du public » et d'« intérêt légitime » qui pourront ouvrir le recours à cette exception.

- **Qu'est-ce qu'un transfert nécessaire à l'exécution d'un contrat entre le responsable du traitement et l'intéressé ou de mesures pré-contractuelles prises à la demande de celui-ci ?**

Dans son document de travail WP 114, le groupe de l'article 29 a précisé qu'un transfert de données ne peut reposer sur cette dérogation que dans la mesure où une « connexion réelle et substantielle » est établie entre ce transfert et l'exécution du contrat concerné ou de mesures pré-contractuelles prises à la demande de la personne.

Il en est déduit qu'il serait illégitime d'invoquer cette exception pour fonder le transfert de données relatives aux salariés de leurs filiale vers la maison-mère d'un groupe multinational, notamment aux fins de centralisation des activités de gestion de la paie et des ressources humaines pour l'ensemble du groupe, au motif que le transfert pourrait être considéré comme nécessaire à l'exécution du contrat de travail conclu entre le salarié et le responsable de traitement.



La notion d’exécution du contrat de travail ne pouvant être interprétée d’une façon aussi large : aucun lien direct et objectif n’existe entre l’exécution d’un contrat de travail et un tel transfert.

Le caractère supposé nécessaire d’un transfert vers une société étrangère pour l’exécution de contrats conclus par un responsable de traitement établi dans l’Union européenne est d’ailleurs, en règle générale, purement subjectif. Il résulte généralement d’un choix économique et/ou organisationnel, c'est à dire d’une décision interne à l’organisation concernée, et non d’une nécessité objective qui serait imposée, par exemple, par une disposition législative nationale. Ce critère de nécessité objective correspond à l’interprétation du Groupe de l’article 29 des exceptions relatives à l’exécution du contrat dans ses documents de travail WP 12 et WP114.

Par ailleurs, une interprétation stricte de cette exception implique que les données transférées doivent être strictement nécessaires et proportionnées à la finalité de l’exécution de ce contrat ou de ces mesures pré-contractuelles.

Il sera dès lors impossible de recourir à cette exception pour transférer des données supplémentaires non essentielles à la finalité du transfert, ou si le transfert n’a pas pour objet l’exécution du contrat mais répond à une autre finalité.

- **Qu’est-ce qu’un transfert nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers ?**

Dans son document de travail WP 114, le groupe de l’article 29 a précisé qu’un transfert ne peut reposer sur cette dérogation que dans la mesure où une « connexion réelle et substantielle » est établie entre ce transfert et la conclusion ou à l’exécution d’un contrat passé entre le responsable de traitement et un tiers, dans l’intérêt de la personne concernée.

Ainsi, à titre d’exemple, l’on peut imaginer que cette condition s’applique dans un cas où une personne située sur le territoire de l’Union européenne se porte acquéreur d’un bien immobilier situé dans un pays tiers ; ses données personnelles pourront alors librement être transférées vers le vendeur, établi dans un pays tiers, par l’agent immobilier, situé en Europe, qui a été chargé de gérer cette acquisition.

La CNIL est fréquemment interrogée sur le fait que de savoir si cette dérogation trouverait à s’appliquer dans le cadre de la gestion de programmes de stock-options nécessitant le recours à des prestataires financiers spécialisés, établis dans des pays tiers.

La CNIL est réservée sur la validité de cette interprétation. En effet, le choix de ce prestataire établi dans un pays tiers ne répond pas *a priori* au critère de « connexion réelle et substantielle » ou de « nécessité objective » qu’il convient d’appliquer dans ces cas.

Par ailleurs, il est ici opportun de rappeler que la régularité des transferts impliqués dans de telles situations imposerait au contraire qu’ils soient encadrés de manière précise. La circonstance particulière dans laquelle le transfert aurait lieu au bénéfice de la personne concernée n’apparaît donc pas davantage pertinente à cet égard.



Quelles sont les formalités à accomplir auprès de la CNIL en matière de transferts internationaux de données ?

Attention : des dispositions réglementaires doivent venir préciser les dispositions de la loi sur les procédures à respecter auprès de la CNIL en matière de transferts internationaux de données. Cette FAQ sera mise à jour dès la parution du décret.

Les formalités à accomplir auprès de la CNIL en matière de transferts internationaux doivent s'articuler avec les formalités relatives au traitement principal dont le transfert est issu.

Si le traitement principal doit faire l'objet d'une déclaration ordinaire auprès de la CNIL (article 23 de la loi du 6 janvier 1978), la déclaration devra préciser qu'un transfert de données a lieu vers un pays non-membre de l'Union européenne (question 6 du formulaire de déclaration normale).

Dans ce cas, le déclarant devra remplir une annexe spécifique relative au transfert. Le modèle d'annexe type peut être téléchargée sur la page « déclaration » du site de la CNIL.

Le transfert, s'il est basé sur un contrat ou des règles internes, fera l'objet d'une autorisation par la CNIL.

Cas particuliers :

1. Le cas des traitements exonérés de déclaration du fait de la désignation d'un correspondant « Informatique et Libertés »

La loi prévoit que la désignation d'un correspondant à la protection des données ou correspondant « Informatique et Libertés » (CIL) par le responsable de traitement a pour effet de dispenser celui-ci de l'accomplissement des formalités prévues aux articles 23 *(déclaration)* et 24 *(déclaration simplifiée)*. Cette exonération ne s'applique pas, cependant, aux autorisations de transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne. Dans certains cas, les transferts devront ainsi faire l'objet d'une autorisation par la CNIL.

Cependant, lorsque les dossiers de transferts sont présentés par un correspondant, la CNIL les examine en priorité.

2. Le cas des transferts issus de traitements relevant du champ d'application d'une norme simplifiée

Les normes simplifiées adoptées par la CNIL sont d'interprétation stricte. Ainsi, si elles ne précisent pas expressément que des traitements dont sont issus les transferts de données vers des pays n'appartenant pas à l'Union européenne rentrent dans leur champ d'application, les traitements faisant l'objet de tels transferts devront faire l'objet d'une déclaration ordinaire. Si ces transferts sont basés sur des contrats ou des règles internes, les transferts devront faire l'objet d'une autorisation spécifique par la CNIL.

Cas particuliers :

> Les normes simplifiées 48 et 46 ont été étendues par deux délibérations du 17 novembre 2005 pour permettre aux responsables de traitement de bénéficier de ces mesures de formalités allégées y compris quand des transferts hors CE seraient issus des traitements couverts par ces normes.

Attention : cette extension n'est pas générale. Elle est soumise à condition et ne vaut que pour certaines des finalités visées par ces normes. Vérifiez soigneusement si cette extension vous est bien applicable.

Les délibérations correspondantes sont disponibles sur le site de la CNIL (version consolidée):

- Délibération n° 2005-276 portant modification de la norme simplifiée n° 48 concernant les traitements automatisés de données à caractère personnel relatifs à la gestion des fichiers de clients et de prospects
- Délibération n° 2005-277 modifiant la norme simplifiée n° 46 destinée à simplifier l'obligation de déclaration des traitements mis en oeuvre par les organismes publics et privés pour la gestion de leurs personnels



Annexes

- **Annexe 6 (Complément de la rubrique 6 du formulaire de déclaration)**
- **Tableau de concordance entre les clauses types émises par la Commission européenne le 15 juin 2001 et les clauses d'un contrat alternatif**



Annexe 6

- **Transfert d'informations entre le territoire français et l'étranger (hors Union Européenne)**

(Complément de la rubrique 6 du formulaire)

(Cette annexe concerne les transmissions effectuées par voie informatique ou sur support papier).

Important : La décision d'autorisation que la CNIL doit délivrer sur les transferts internationaux de données en application de l'article 69 al. 8 de la loi du 6 janvier 1978 sont prises sur la base des informations renseignées dans cette annexe.

Dans le cas de transfert de données entre le territoire français et le territoire d'Etats n'appartenant pas à l'Union européenne, indiquez :

L'identité de la société déclarante (éventuellement, le nom du groupe à laquelle elle appartient)	
Le numéro de dossier attribué par la CNIL (si vous disposez déjà d'un tel numéro)	Dossier n°
La finalité du traitement principal	
La finalité du transfert	
L'identité du destinataire	
Le pays d'établissement du destinataire	
La nature des traitements opérés chez le destinataire	
Les catégories de personnes concernées par le transfert *	



Les catégories de données transférées ∗	
La ou les catégories de destinataires ∗	
La durée de conservation des données chez le destinataire	
La nature des garanties mises en œuvre par le destinataire des données visant à assurer un niveau de protection suffisant au regard de la protection des données transférées (ex: contrat, règles internes) – (joindre copie des documents concernés au dossier) ∗∗ :	
La nature et les modalités d'information des personnes concernées (information individuelle et/ou collective)	

∗ Si le transfert a plusieurs finalités, ces informations doivent être fournies de manière distincte pour chacune d'entre elles.

∗∗ Cette information ne sera nécessaire que si le pays de destination n'a pas été reconnu par la Commission Européenne comme accordant une protection adéquate. La liste mise à jour des pays accordant une protection adéquate est publiée sur le site de la CNIL (« dossier International »).



- **Tableau de concordance entre les clauses types émises par la Commission européenne le 15 juin 2001 et les clauses d'un contrat alternatif**

(transfert de responsable de traitement à responsable de traitement)

Ce tableau peut être utilisé pour apprécier si les garanties offertes par un contrat de transfert de responsable de traitement à un responsable de traitement serait suffisant, dès lors qu'il n'est pas basé sur les clauses contractuelles types.

Il convient de préciser en face de chacune des rubriques précisées dans la colonne de gauche quel est l'équivalent de la clause décrite dans le contrat soumis à la CNIL (si elle existe).

Clauses contractuelles types du 15 juin 2001	**Contrat soumis à la CNIL**
Clause 1. Informations relatives aux parties **Clause 2. Définitions** **Clause 3. Détails du transfert (annexe 1):** 3.1- personnes concernées 3.2- finalités du transfert 3.3- catégories de données concernées 3.4- données sensibles (le cas échéant) 3.5- destinataires des données 3.6- durées de conservation **Clause 4. Clause de tiers bénéficiaire** (donnant aux personnes concernées le droit de se prévaloir des dispositions du contrat) **Clause 5. Obligations de l'exportateur** *5.1- traitement conforme au droit national (ex : déclaration CNIL ; licéité de la collecte et de la communication à des tiers)* 5.2- si le transfert concerne des catégories spéciales de données, information des personnes sur la transmission de leurs données vers un pays non adéquat *5.3- répondre à la CNIL et/ou aux personnes concernées en cas de questions relatives aux traitements*	



(a) **Clause 6. Obligations de l'importateur**	
6.1- la législation à laquelle il est soumis ne l'empêche pas de respecter les obligations prévues au contrat 6.2- s'engage à traiter les données conformément au droit français <u>OU :</u> 6.3- conformément aux principes énoncés à l'annexe 2 des clauses types, c'est-à-dire : 1. Limitation des transferts à une finalité spécifique 2. Qualité et proportionnalité des données 3. Transparence 4. Sécurité et confidentialité 5. Droits d'accès, de rectification, d'effacement et d'opposition 6. Restrictions aux transferts ultérieurs (information extensive des personnes sur la possibilité de transferts ultérieurs, et possibilité de s'y opposer ; dans le cas de données sensibles, le consentement indubitable des personnes est requis) 7. Mesures de protection supplémentaires en cas de transfert de catégories particulières de données 8. Procédures d'opposition efficaces si transfert pour des fins de marketing direct 9. Droit des personnes de ne pas être soumises à des processus de prise de décisions individuelles automatisées 6.4- traitera les demandes de renseignements de l'exportateur ou des personnes concernées quant au traitement 6.5- coopérera avec la CNIL et se rangera à son avis quant au traitement 6.6- à la demande de l'exportateur, se soumettra à un audit par des personnes indépendantes (potentiellement la CNIL) 6.7- mettra à la disposition des personnes une copie des clauses si elles le demandent **Clause 7. Responsabilité conjointe et solidaire**	

envers les personnes concernées **Clause 8. Médiation / juridiction** : quand la personne subit un dommage du fait d'une violation du contrat, les parties acceptent, au choix de la personne, de soumettre le litige à la médiation d'une personne indépendante (potentiellement, la CNIL) OU de porter le litige devant les tribunaux français. **(b)** **(c) Clause 9. Coopération avec la CNIL** *(d) Dépôt d'une copie du contrat à la CNIL (clause inutile car obligatoire en vertu du droit français)* **Clause 10. Résiliation des clauses** : les obligations des parties sont maintenues suite à la résiliation du contrat **(e) Clause 11. Droit applicable : droit français** **Clause 12. Pas de modification unilatérale du contrat**	